Title: Architecture for an Integrated Policy Enforcement System
Inventors: Pankaj S. Parekh, Vimal Vaidya, Sandeep Gupta and Pranav Shah
Atty. Docket No.: 19567-05719

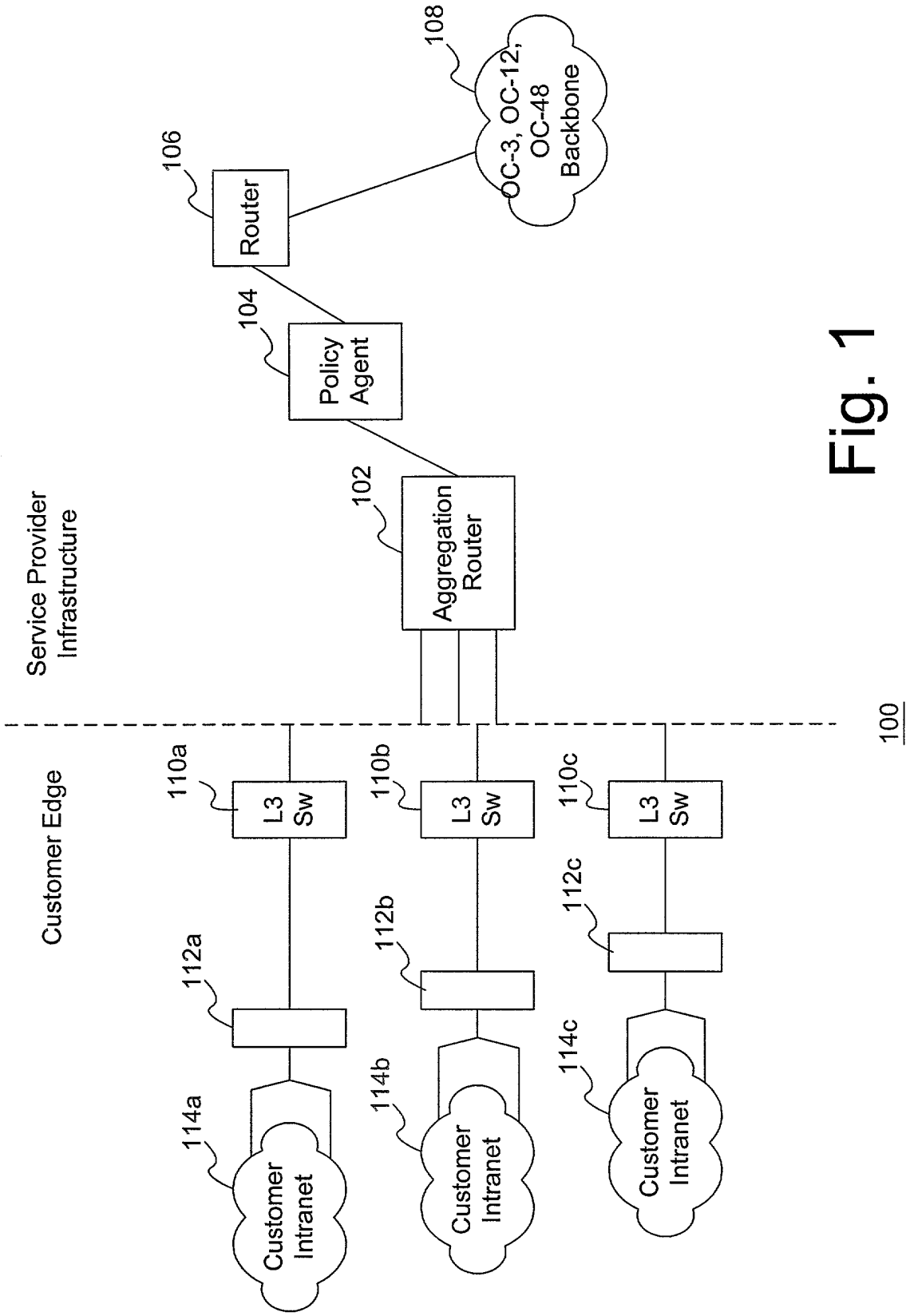

Fig. 1

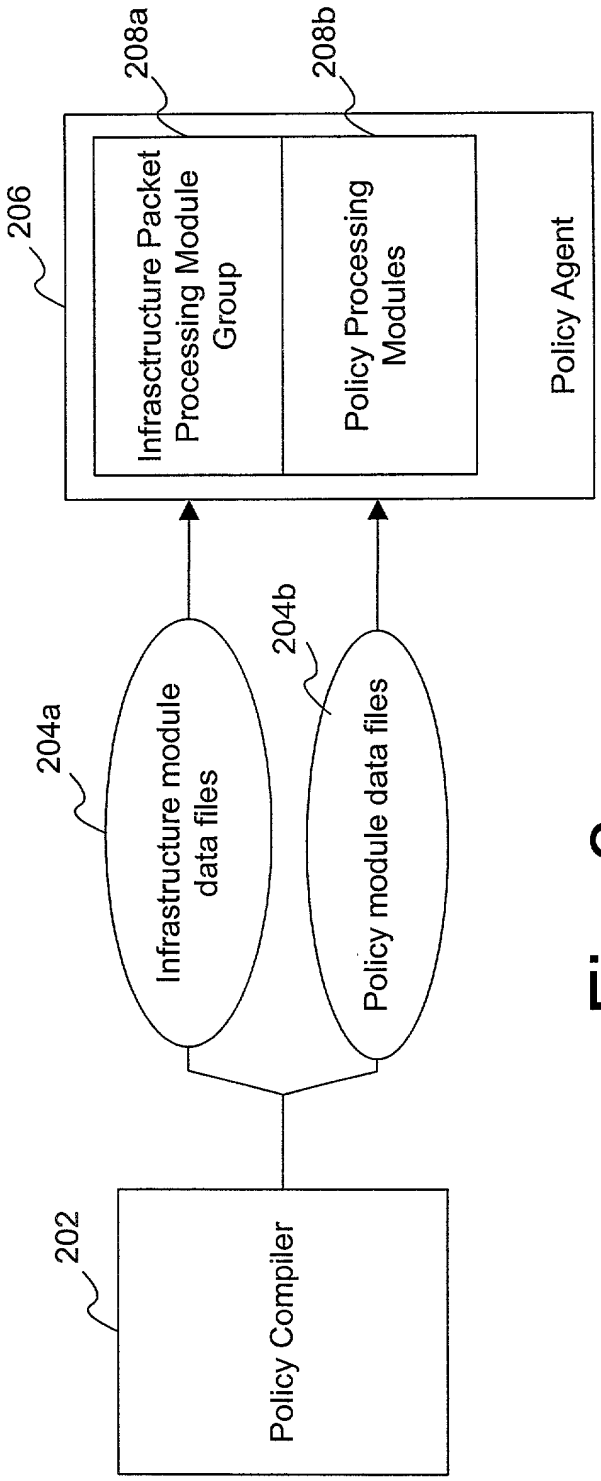
208a
208b
206
Infrastructure Packet Processing Module Group
Policy Processing Modules
Policy Agent
204b
204a
Infrastructure module data files
Policy module data files
202
Policy Compiler

Fig. 2

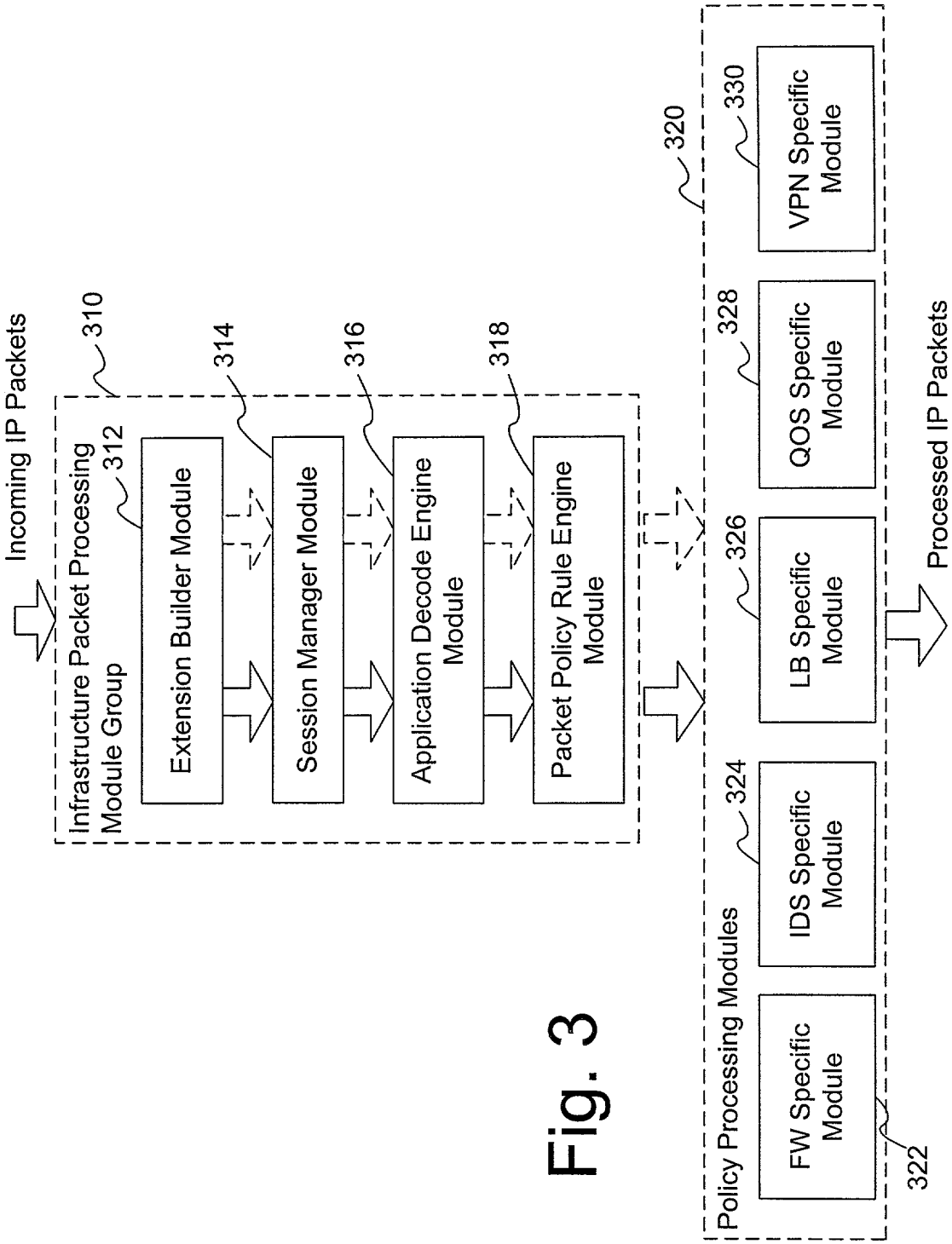
Incoming IP Packets
310
Infrastructure Packet Processing Module Group
312
Extension Builder Module
314
Session Manager Module
316
Application Decode Engine Module
318
Packet Policy Rule Engine Module
320
Policy Processing Modules
322
FW Specific Module
324
IDS Specific Module
326
LB Specific Module
328
QOS Specific Module
330
VPN Specific Module
Processed IP Packets

Fig. 3

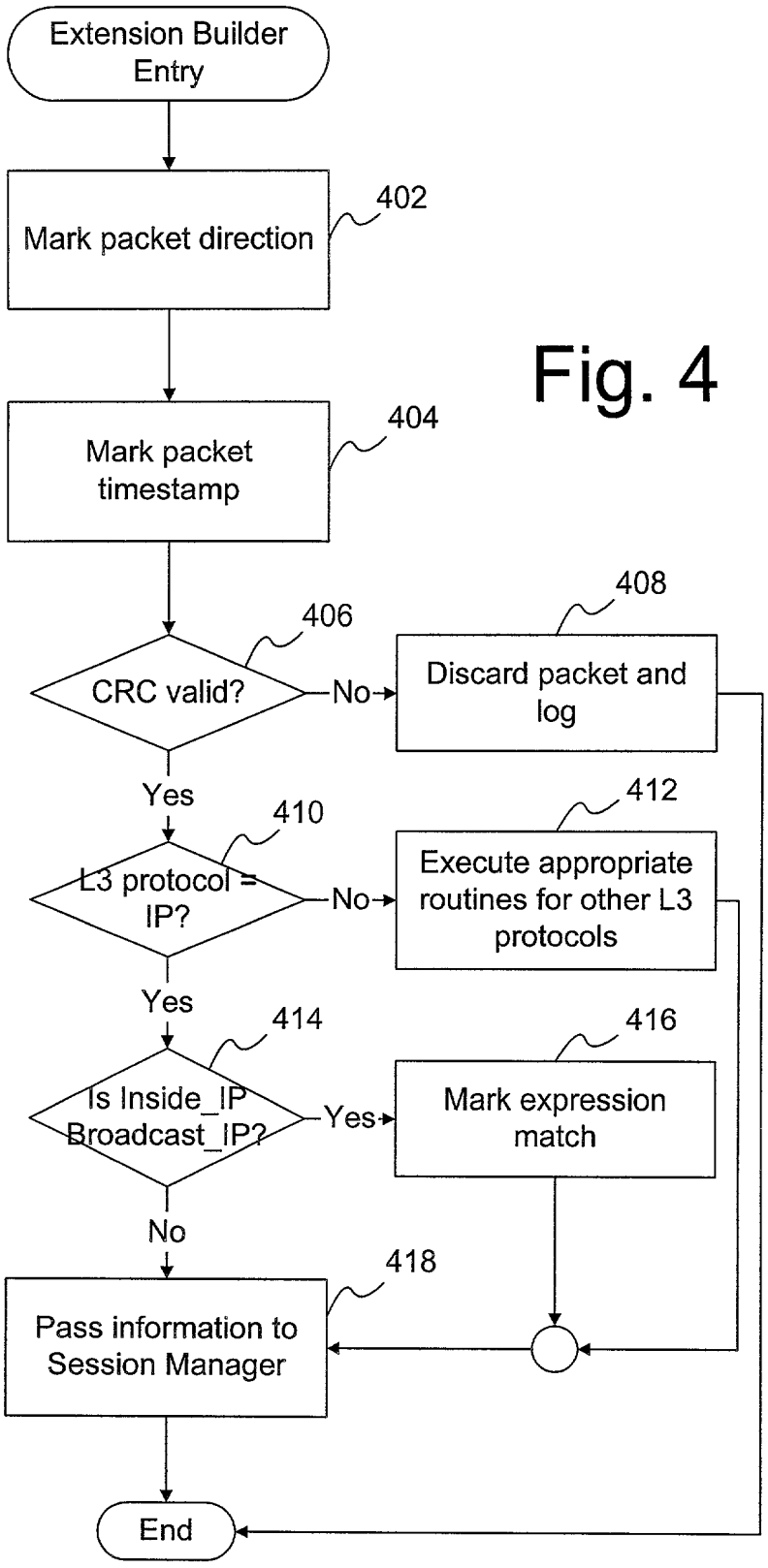
Extension Builder Entry
Mark packet direction
402
Mark packet timestamp
404
CRC valid?
406
No
Discard packet and log
408
Yes
L3 protocol = IP?
410
No
Execute appropriate routines for other L3 protocols
412
Yes
Is Inside_IP Broadcast_IP?
414
Yes
Mark expression match
416
No
Pass information to Session Manager
418
End

Fig. 4

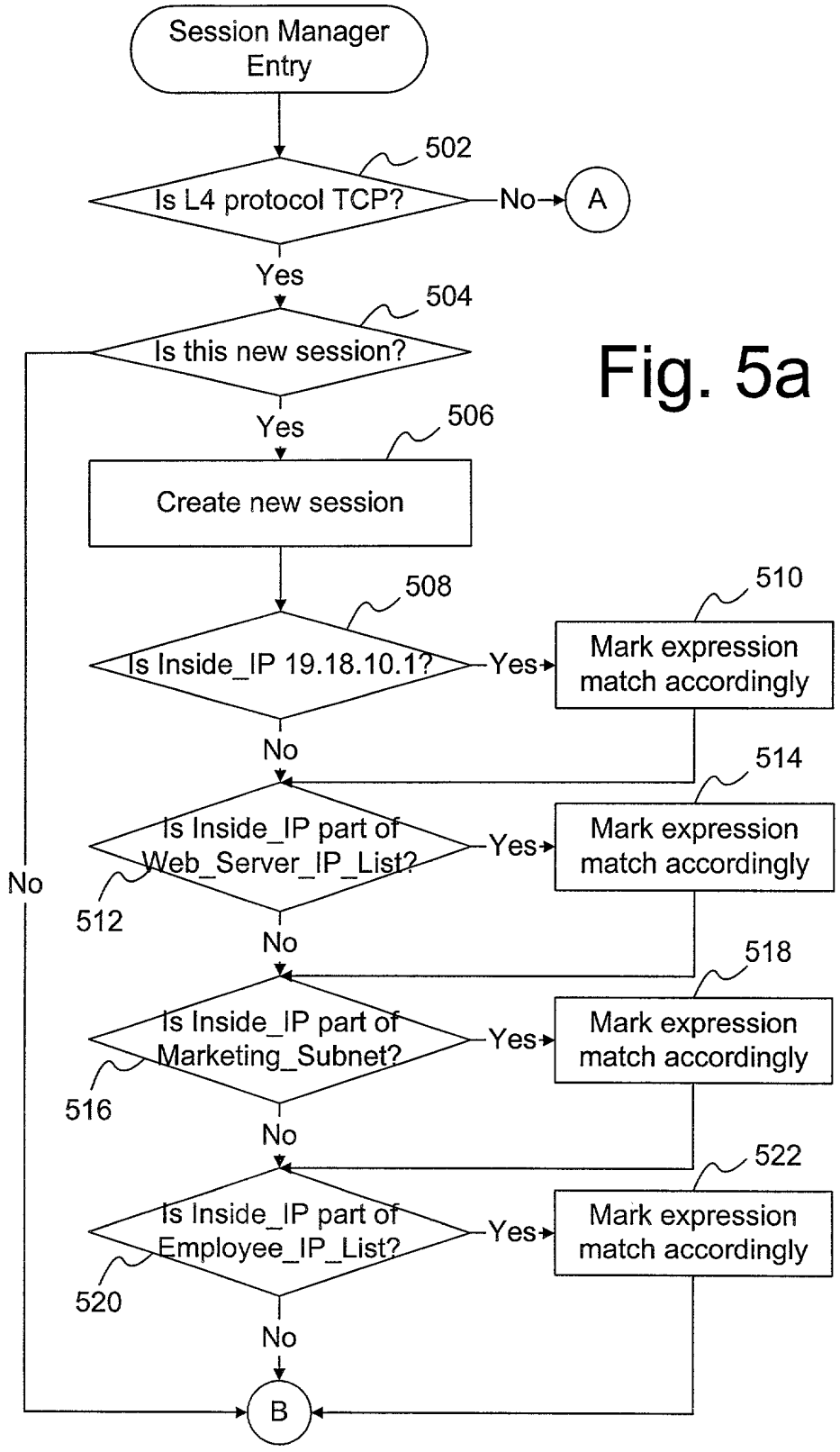
Session Manager Entry
502
Is L4 protocol TCP?
No
A
Yes
504
Is this new session?
Yes
506
Create new session
508
Is Inside_IP 19.18.10.1?
Yes
510
Mark expression match accordingly
No
514
Is Inside_IP part of Web_Server_IP_List?
Yes
Mark expression match accordingly
512
No
518
Is Inside_IP part of Marketing_Subnet?
Yes
Mark expression match accordingly
516
No
522
Is Inside_IP part of Employee_IP_List?
Yes
Mark expression match accordingly
520
No
B
No

Fig. 5a

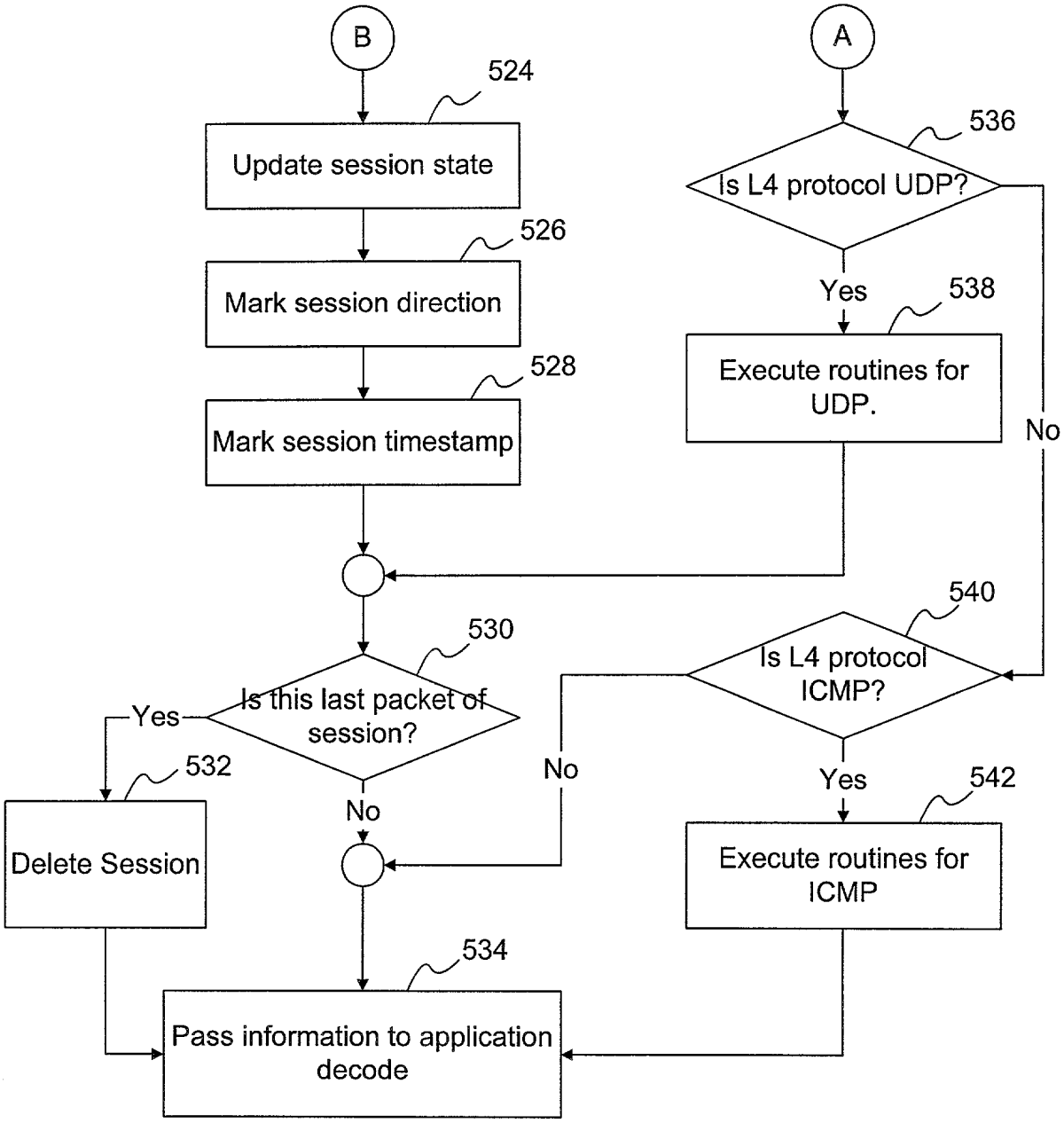
B
524
Update session state
526
Mark session direction
528
Mark session timestamp
530
Is this last packet of session?
Yes
532
Delete Session
No
534
Pass information to application decode
A
536
Is L4 protocol UDP?
Yes
538
Execute routines for UDP.
No
540
Is L4 protocol ICMP?
Yes
542
Execute routines for ICMP
No

Fig. 5b

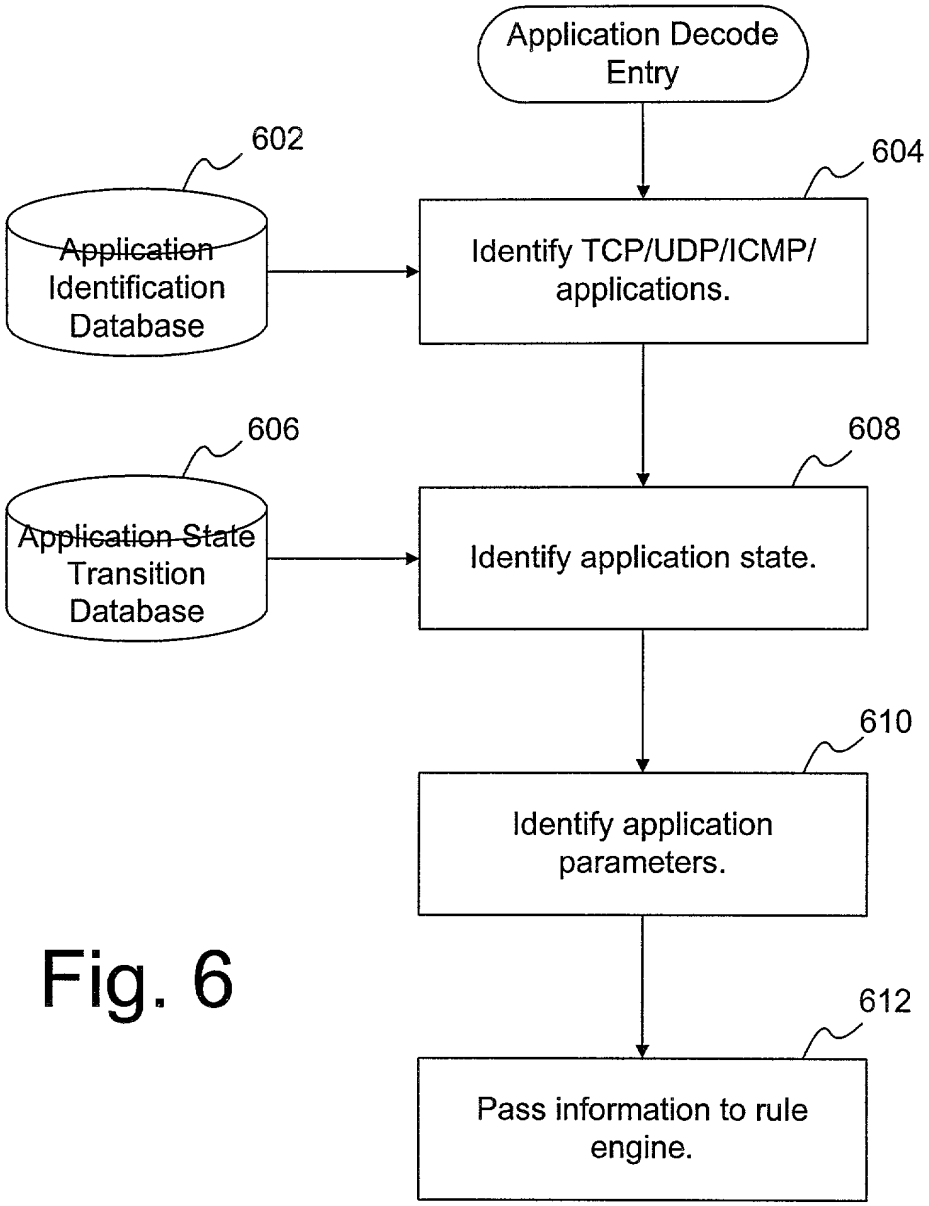
Application Decode Entry
602
604
Application Identification Database
Identify TCP/UDP/ICMP/ applications.
606
608
Application State Transition Database
Identify application state.
610
Identify application parameters.
612
Pass information to rule engine.

Fig. 6

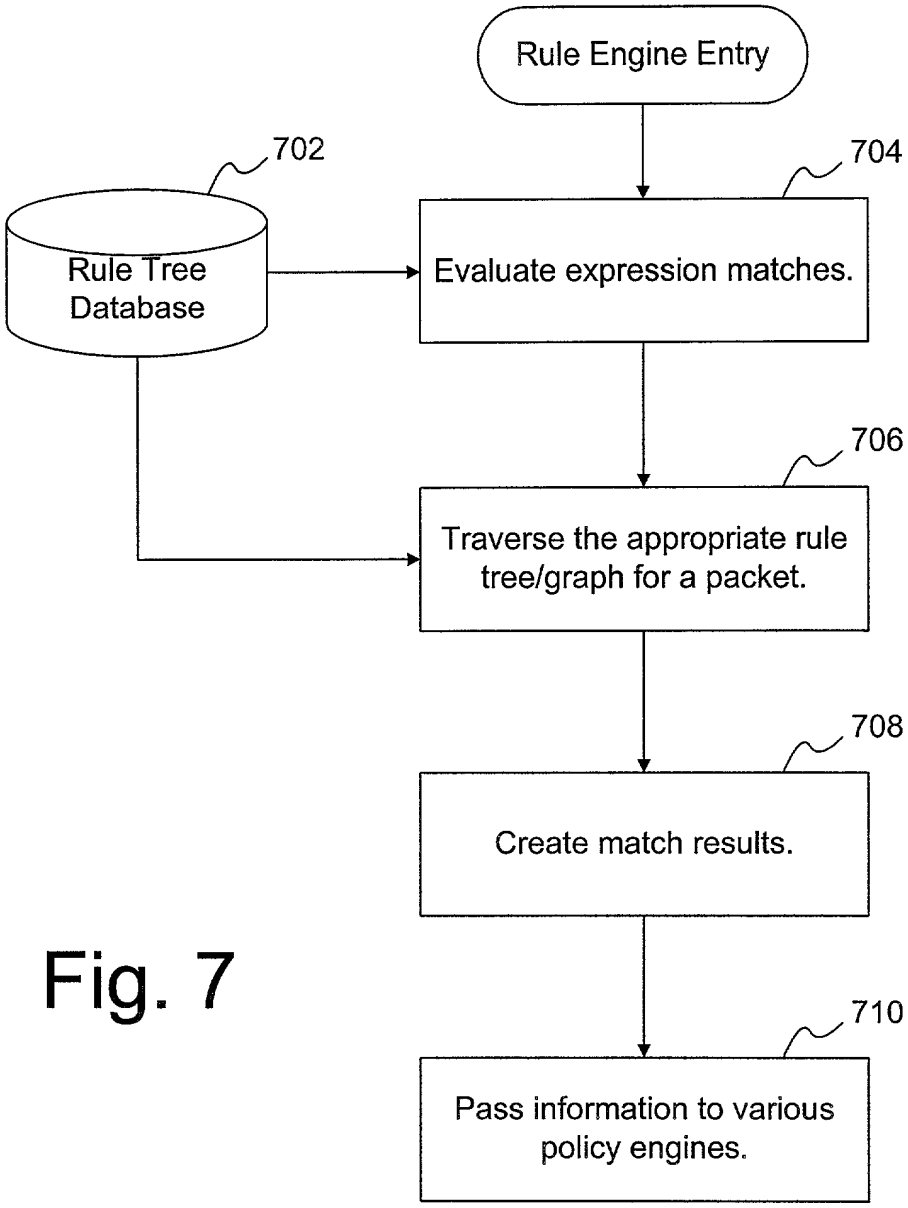
Rule Engine Entry
702
704
Rule Tree Database
Evaluate expression matches.
706
Traverse the appropriate rule tree/graph for a packet.
708
Create match results.
710
Pass information to various policy engines.

Fig. 7

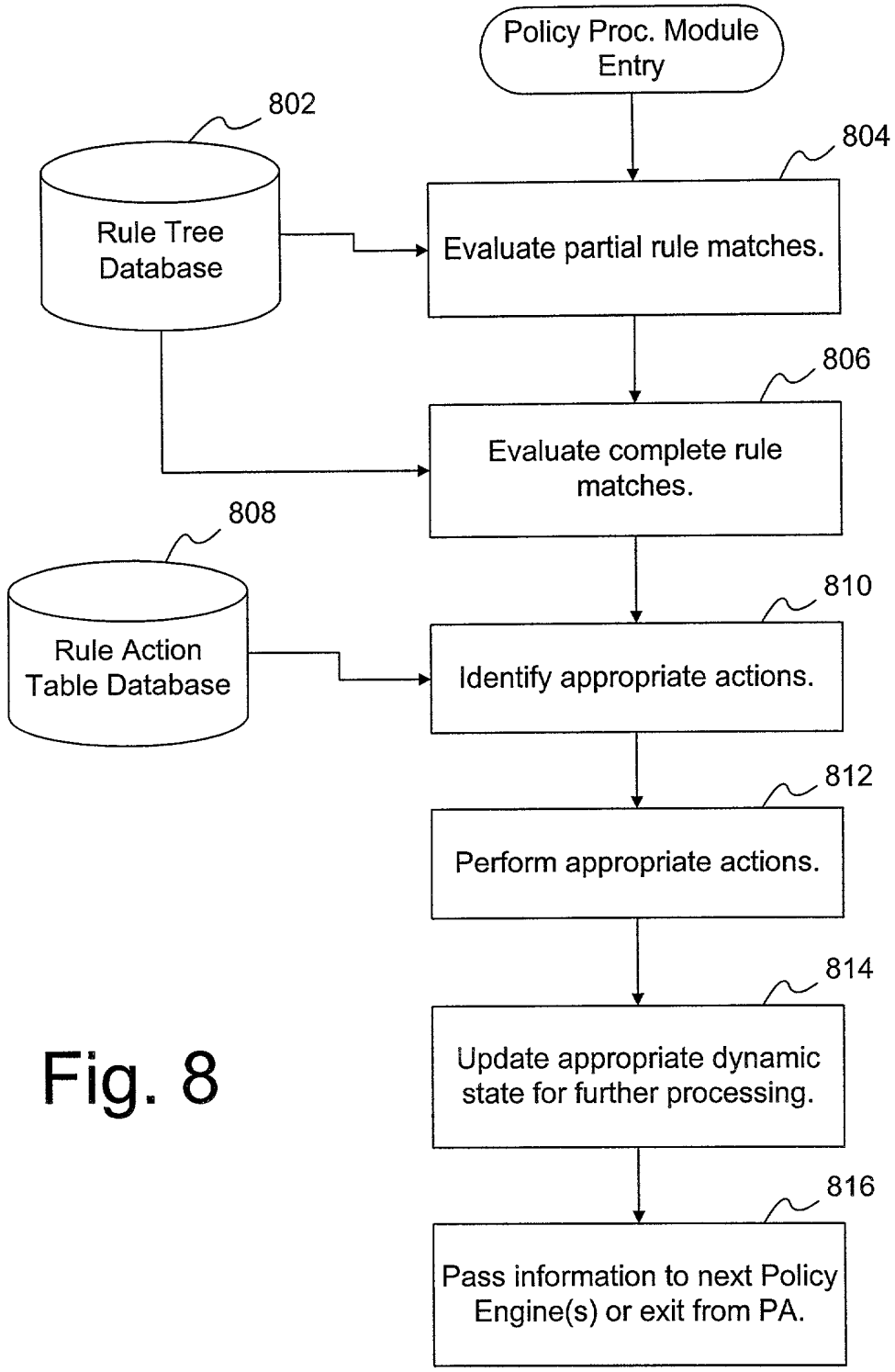
Policy Proc. Module Entry
802
804
Rule Tree Database
Evaluate partial rule matches.
806
Evaluate complete rule matches.
808
810
Rule Action Table Database
Identify appropriate actions.
812
Perform appropriate actions.
814
Update appropriate dynamic state for further processing.
816
Pass information to next Policy Engine(s) or exit from PA.

Fig. 8

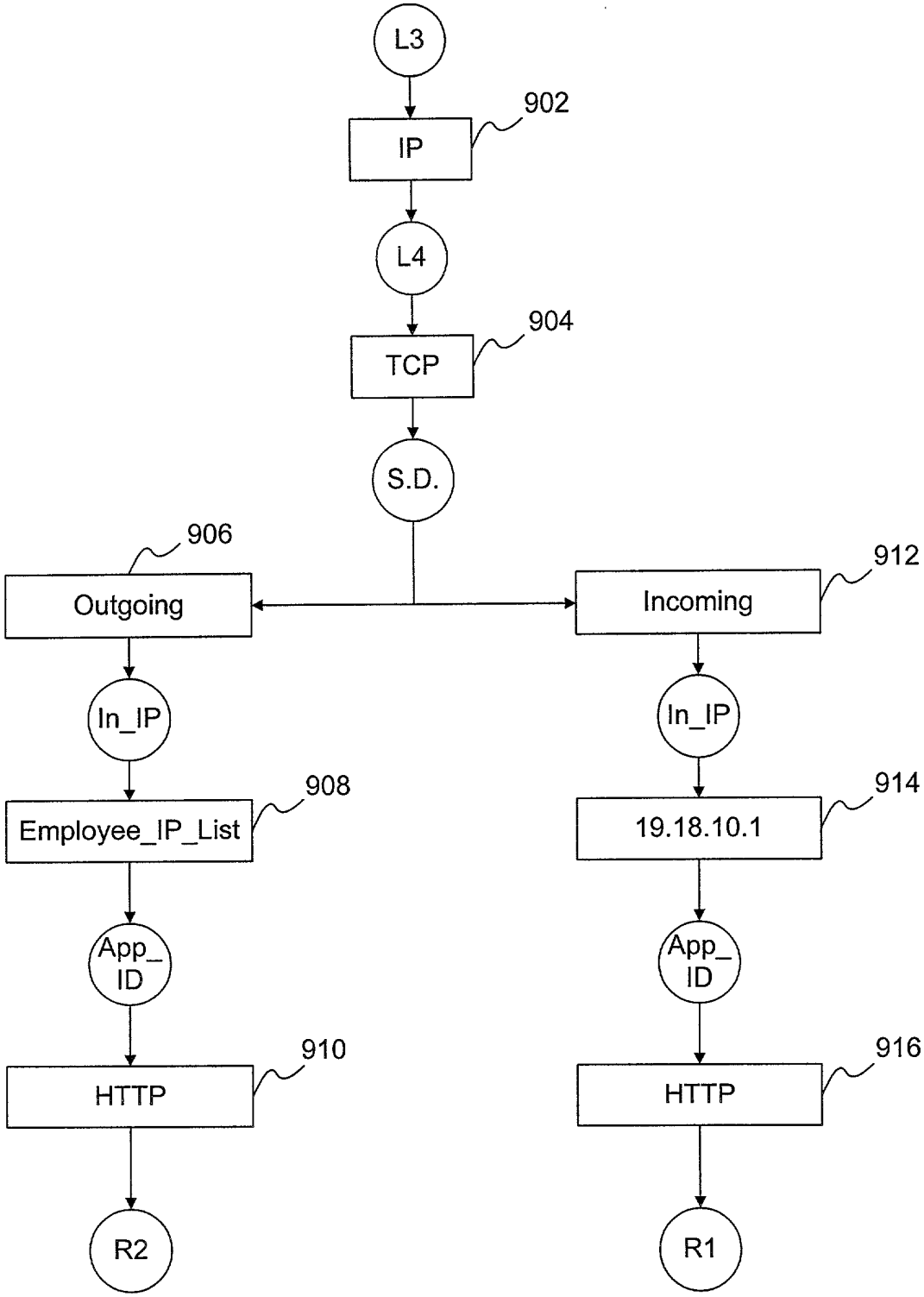
L3
IP
902
L4
TCP
904
S.D.
906
Outgoing
912
Incoming
In_IP
In_IP
908
Employee_IP_List
914
19.18.10.1
App_ ID
App_ ID
910
HTTP
916
HTTP
R2
R1

Fig. 9A

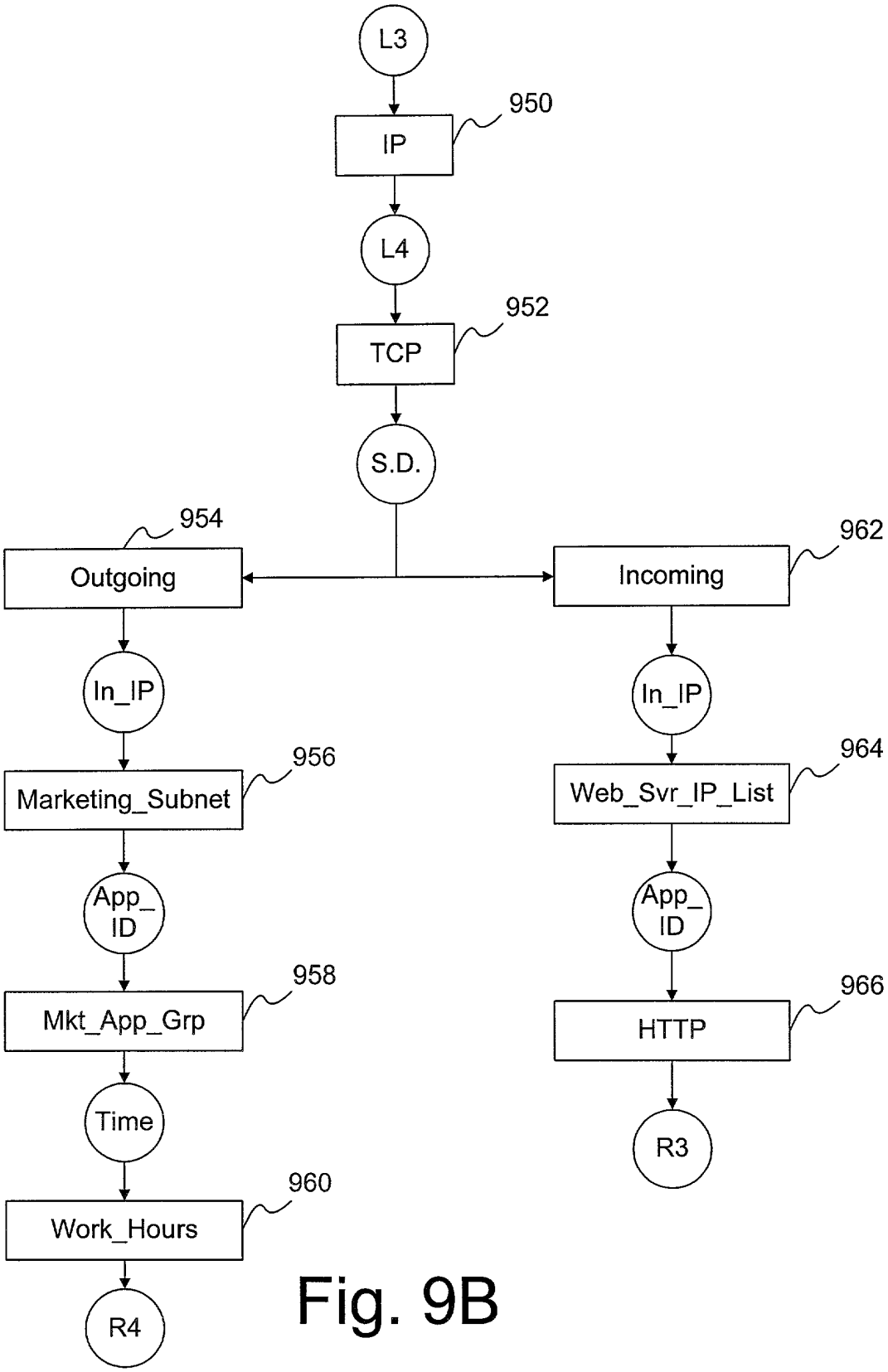
L3
IP
950
L4
TCP
952
S.D.
954
Outgoing
In_IP
Marketing_Subnet
956
App_ ID
Mkt_App_Grp
958
Time
Work_Hours
960
R4
962
Incoming
In_IP
Web_Svr_IP_List
964
App_ ID
HTTP
966
R3

Fig. 9B

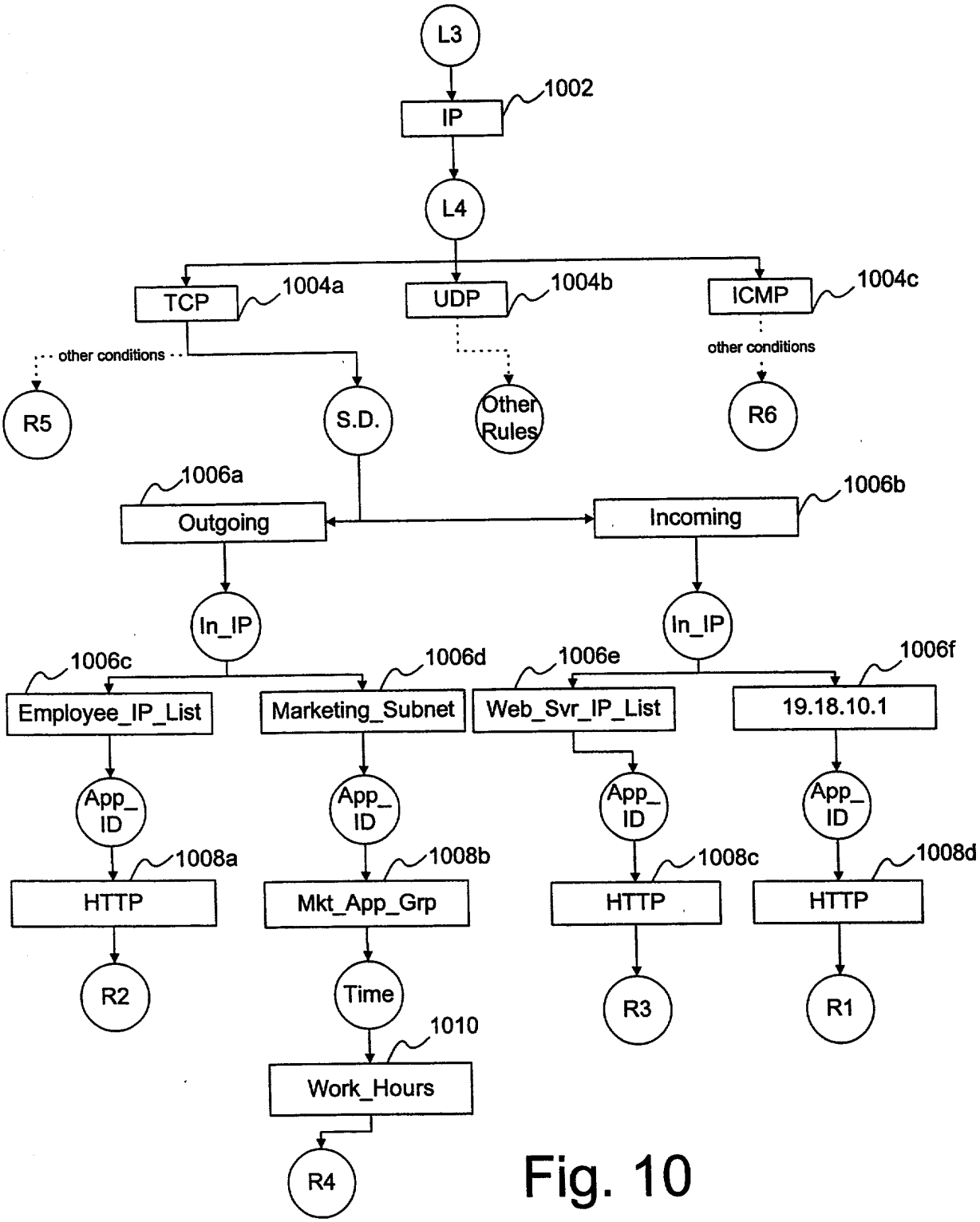
L3
IP
1002
L4
TCP
1004a
UDP
1004b
ICMP
1004c
other conditions
other conditions
R5
S.D.
Other Rules
R6
1006a
Outgoing
Incoming
1006b
In_IP
In_IP
1006c
1006d
1006e
1006f
Employee_IP_List
Marketing_Subnet
Web_Svr_IP_List
19.18.10.1
App_ ID
App_ ID
App_ ID
App_ ID
1008a
1008b
1008c
1008d
HTTP
Mkt_App_Grp
HTTP
HTTP
R2
Time
R3
R1
1010
Work_Hours
R4

Fig. 10